

PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Standard Accounting and Reporting System (STARS)

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

09/28/20

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)

- From members of the general public From Federal employees and/or Federal contractors
 From both members of the general public and Federal employees and/or Federal contractors Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)

- New DoD Information System New Electronic Collection
 Existing DoD Information System Existing Electronic Collection
 Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Standard Accounting and Reporting System (STARS) is a general fund accounting and reporting system used by the Department of Navy (DON) Major Commands. The system provides the capability to record and execute budgetary and accounting events from funds allocation to disbursement. STARS also serves as a primary reporting source of DON funds status and execution for departmental reporting purposes.

STARS contains names and full and truncated Social Security Numbers (SSNs). The information is sent to STARS through file transfers from another Defense Finance and Accounting Service (DFAS) and Navy accounting and pay entitlement systems. This information is maintained within STARS and cannot be retrieved using a personal identifier.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

PII is collected for verification, mission related use, and data matching.

e. Do individuals have the opportunity to object to the collection of their PII? Yes No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

The STARS feeder system Defense Civilian Pay System (DCPS) procedures provide individuals with the opportunity to object to the collection of the information, but STARS does not because PII is interfaced into the system via a partner. Therefore, STARS is not required to provide the opportunity for users to object to the collection of their PII.

f. Do individuals have the opportunity to consent to the specific uses of their PII? Yes No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Information is stored in STARS, without direct retrieval. Information collected in STARS is solely to record obligations for labor costs. This information is maintained within STARS and cannot be retrieved using a personal identifier.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

- Privacy Act Statement Privacy Advisory Not Applicable

THIS SYSTEM CONTAINS PRIVACY ACT DATA

AUTHORITY: EXECUTIVE ORDER 10450, 9397, AND PUBLIC LAW 99-474, THE COMPUTER FRAUD AND ABUSE ACT
PURPOSE OF USE: TO RECORD NAMES AND SOCIAL SECURITY NUMBERS FOR THE PURPOSE OF VALIDATING THE TRUSTWORTHINESS OF INDIVIDUALS REQUESTING ACCESS TO DEPARTMENT OF DEFENSE (DOD) SYSTEMS AND INFORMATION.

ROUTINE USES: THOSE GENERALLY PERMITTED UNDER THE 5 U.S.C. 522A(B) OF THE PRIVACY ACT AS REQUIRED.
DISCLOSURE: DISCLOSURE OF THIS INFORMATION IS VOLUNTARY; HOWEVER, FAILURE TO PROVIDE THE REQUESTED INFORMATION MAY IMPEDE, DELAY OR PREVENT FURTHER PROCESSING OF THIS REQUEST.

NOTE: RECORDS MAY BE MAINTAINED IN BOTH ELECTRONIC AND/OR PAPER FORM.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

- Within the DoD Component Specify.
- Other DoD Components Specify.
- Other Federal Agencies Specify.
- State and Local Agencies Specify.
- Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.) Specify.
- Other (e.g., commercial providers, colleges). Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

- Individuals Databases
- Existing DoD Information Systems Commercial Systems
- Other Federal Information Systems

Defense Civilian Pay System (DCPS)

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- E-mail Official Form (Enter Form Number(s) in the box below)
- Face-to-Face Contact Paper
- Fax Telephone Interview
- Information Sharing - System to System Website/E-Form
- Other (If Other, enter the information in the box below)

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

- Yes No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcltd.defense.gov/Privacy/SORNs/>
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

The PII within STARS is not retrieved by name or unique identifier. PII is only stored to record obligations. This information is maintained within the STARS system and cannot be retrieved using a personal identifier.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority

for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

DFAS 5015.2-M

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

DFAS 5015.2-I, Records Management Procedures,
DFAS 5015.2-M, Records Disposition Schedules, and
Cutoff at the end of the fiscal year and destroy 10 years after cutoff.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).
 - (a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
 - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.
 - (c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

In Accordance With IAW DFAS Instruction 8500.01-I, 5 U.S.C. 301, Departmental Regulations; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R, Vol. 5; 31 U.S.C. Sections 3511, Prescribing accounting requirements and developing accounting systems; Section 3512, Executive agency accounting and other financial management reports and plans; 31 U.S.C. 3513, Finance Reporting and Accounting System; and E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes No Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

STARS does not collect information from the public. STARS information is collected via interface partners.

SECTION 2: PII RISK REVIEW

a. What PII will be collected (a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)

- | | | |
|---|---|--|
| <input type="checkbox"/> Biometrics | <input type="checkbox"/> Birth Date | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Disability Information | <input type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input type="checkbox"/> Education Information | <input type="checkbox"/> Emergency Contact |
| <input type="checkbox"/> Employment Information | <input type="checkbox"/> Financial Information | <input type="checkbox"/> Gender/Gender Identification |
| <input type="checkbox"/> Home/Cell Phone | <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Legal Status |
| <input type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Marital Status | <input type="checkbox"/> Medical Information |
| <input type="checkbox"/> Military Records | <input type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input type="checkbox"/> Official Duty Address | <input type="checkbox"/> Official Duty Telephone Number | <input type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Passport Information | <input type="checkbox"/> Personal E-mail Address | <input type="checkbox"/> Photo |
| <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Position/Title | <input type="checkbox"/> Protected Health Information (PHI) ¹ |
| <input type="checkbox"/> Race/Ethnicity | <input type="checkbox"/> Rank/Grade | <input type="checkbox"/> Religious Preference |
| <input type="checkbox"/> Records | <input type="checkbox"/> Security Information | <input checked="" type="checkbox"/> Social Security Number (SSN) (Full or in any form) |
| <input type="checkbox"/> Work E-mail Address | <input type="checkbox"/> If Other, enter the information in the box below | |

N/A

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

- Yes No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

STARS is currently creating a justification memo to submit to the DFAS privacy office.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Identification. The information is collected in STARS to record obligations for labor costs to research and validate accurate pay entitlements to civilians. The travel information is collected for specific travel orders to verify traveler entitlement amounts are correct. This information is maintained within the STARS system and cannot be retrieved using a personal identifier.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

STARS does not use SSNs for reporting purposes on the DON financial statements (i.e. system objections). STARS is also a legacy system that is scheduled to be decommissioned in the next few years and no major System Change Requests (SCR's) will be approved; therefore, a mitigation strategy has not been developed.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?

If "No," explain.

- Yes No

PII is required for mission-related use for our DCPS interface partner.

b. What is the PII confidentiality impact level²?

- Low Moderate High

¹The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

²Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically

conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- | | |
|---|---|
| <input checked="" type="checkbox"/> Cipher Locks | <input checked="" type="checkbox"/> Closed Circuit TV (CCTV) |
| <input checked="" type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges |
| <input checked="" type="checkbox"/> Key Cards | <input type="checkbox"/> Safes |
| <input checked="" type="checkbox"/> Security Guards | <input type="checkbox"/> If Other, enter the information in the box below |

(2) Administrative Controls. *(Check all that apply)*

- Backups Secured Off-site
- Encryption of Backups
- Methods to Ensure Only Authorized Personnel Access to PII
- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- If Other, enter the information in the box below

(3) Technical Controls. *(Check all that apply)*

- | | | |
|---|---|--|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Common Access Card (CAC) | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest | <input checked="" type="checkbox"/> Encryption of Data in Transit | <input type="checkbox"/> External Certificate Authority Certificates |
| <input checked="" type="checkbox"/> Firewall | <input checked="" type="checkbox"/> Intrusion Detection System (IDS) | <input checked="" type="checkbox"/> Least Privilege Access |
| <input checked="" type="checkbox"/> Role-Based Access Controls | <input checked="" type="checkbox"/> Used Only for Privileged (Elevated Roles) | <input checked="" type="checkbox"/> User Identification and Password |
| <input checked="" type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> If Other, enter the information in the box below | |

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

STARS has implemented a continuous monitoring strategy that includes annual FISMA and MICP-IT FISCAM testing. STARS also performs quarterly privileged user reviews and annual authorized user reviews.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool³?

<input checked="" type="checkbox"/> Yes, DITPR	DITPR System Identification Number	<input type="text" value="5"/>
<input type="checkbox"/> Yes, SIPRNET	SIPRNET Identification Number	<input type="text"/>
<input checked="" type="checkbox"/> Yes, RMF tool	RMF tool Identification Number	<input type="text" value="82"/>
<input type="checkbox"/> No		

If "No," explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology".

Indicate the assessment and authorization status:

<input checked="" type="checkbox"/> Authorization to Operate (ATO)	Date Granted: <input type="text" value="8/26/2020"/>
<input type="checkbox"/> ATO with Conditions	Date Granted: <input type="text"/>
<input type="checkbox"/> Denial of Authorization to Operate (DATO)	Date Granted: <input type="text"/>
<input type="checkbox"/> Interim Authorization to Test (IATT)	Date Granted: <input type="text"/>

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

Yes No

If "Yes," Enter UII If unsure, consult the component IT Budget Point of Contact to obtain the UII

³Guidance on Risk Management Framework (RMF) tools (i.g., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at <https://rmfks.osd.mil>.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Janine Graham	(1) Title	System Manager	
	(2) Organization	ZTCCA	(3) Work Telephone	216-204-2866
	(4) DSN		(5) E-mail address	JANINE.A.GRAHAM.CIV@MAIL.MIL
	(6) Date of Review	09/12/19	(7) Signature	
b. Other Official (to be used at Component discretion)	Ashley Pierson	(1) Title	Information System Security Manager	
	(2) Organization	ZTCCB	(3) Work Telephone	216-204-4331
	(4) DSN		(5) E-mail address	ASHLEY.L.PIERSON.CIV@MAIL.MIL
	(6) Date of Review	09/12/19	(7) Signature	
c. Other Official (to be used at Component discretion)		(1) Title		
	(2) Organization		(3) Work Telephone	
	(4) DSN		(5) E-mail address	
	(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)	Gregory L. Outlaw	(1) Title	Privacy Officer	
	(2) Organization	ZC	(3) Work Telephone	(317) 212-4591
	(4) DSN	699-4591	(5) E-mail address	GREGORY.L.OUTLAW.CIV@MAIL.MIL
	(6) Date of Review	01/29/20	(7) Signature	

e. Component Records Officer	Ralph Mullins	(1) Title	Agency Records Manager
(2) Organization	ZED	(3) Work Telephone	317-212-7775
(4) DSN		(5) E-mail address	ralph.e.mullins.civ@mail.mil
(6) Date of Review	01/30/20	(7) Signature	
f. Component Senior Information Security Officer or Designee Name	Jack Schiller	(1) Title	Deputy Director, IT Shared Services
(2) Organization	ZTA	(3) Work Telephone	317-212-1808
(4) DSN		(5) E-mail address	jack.j.schiller.civ@mail.mil
(6) Date of Review:	09/21/20	(7) Signature	
g. Senior Component Official for Privacy (SCOP) or Designee Name	Angela R. Schultz	(1) Title	Corporate Communications Director
(2) Organization	ZC	(3) Work Telephone	317-212-6195
(4) DSN		(5) E-mail address	angela.r.schultz6.civ@mail.mil
(6) Date of Review	02/20/20	(7) Signature	
h. Component CIO Reviewing Official Name	Paul Gass	(1) Title	Chief Information Officer
(2) Organization	ZT	(3) Work Telephone	317-212-4800
(4) DSN		(5) E-mail address	gregory.p.gass2.civ@mail.mil
(6) Date of Review		(7) Signature	

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.